

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

08/27/2019

**SUBJECT:**

A Vulnerability in Apple iOS Could Allow for Arbitrary Code Execution

**OVERVIEW:**

A vulnerability has been discovered in Apple iOS, which could allow for arbitrary code execution. Apple iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch. Successful exploitation of this vulnerability could result in arbitrary code execution with system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- iOS versions prior to 12.4.1

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: HIGH**

**TECHNICAL SUMMARY:**

A vulnerability has been discovered in Apple iOS, which if exploited could allow for arbitrary code execution with system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The vulnerability exists due to a use-after-free error. Specifically, this issue occurs due to stale pointer left by 'in6\_pcbdetach()' function.

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.

- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.

**REFERENCES:**

**Apple:**

<https://support.apple.com/en-us/HT210549>

**CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8605>

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<http://www.us-cert.gov/tlp/>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

**Chris Watts**

Security Operations Analyst

MS Department of Information Technology Services

601-432-8201 | [www.its.ms.gov](http://www.its.ms.gov)



DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited